Welcome to the ARES 2010 Conference

February, 15th - 18th 2010
Andrzej Frycz Modrzewski Cracow College
Krakow,Poland

***** ATTENTION *****

The final program is available. Please note that changes may occur!

The registration desk opens at 08:00.

The Fifth International Conference on Availability, Reliability and Security ("ARES 2010 – The International Dependability Conference") will bring together researchers and practitioners in the area of dependability. ARES 2010 will highlight the various aspects of dependability - with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of the research issues of dependability as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.

ARES will emphasize the interplay between foundations and practical issues of dependability in emerging areas such as e-government, m-government, location-based applications, ubiquitous computing, autonomous computing, chances of grid computing etc.

ARES is devoted to the critical examination and research challenges of the various aspects of Dependable Computing and the definition of a future road map.

Selected papers that are accepted by and presented at the ARES Conference will be published, after further revision, in

special issues of internationa journals. Papers of ARES 2009 were selected to appear in special issues of the journals (JISSec, IJCCBS).

The acceptance rate of the ARES 2009 conference was 25%. More information about previous ARES conference can be found here: >>previous conferences<< .

We are proud to announce Ross Anderson and Gene Spafford as keynote speakers of ARES 2010: >>keynotes<<

The ARES 2010 conference is...

... organized by

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

2010 International Conference on Availability, Reliability and Security

ARES 2010

Table of Contents

ARES 2010 Full Papers

Network Security I

Network Security II

Identity Management, Authentication, and Authorization I

Identity Management, Authentication, and Authorization II

Availability and Reliability I

Availability and Reliability II

Risk and Security Management I

Risk and Security Management II

Risk and Security Management III

ARES 2010 Short Papers

Security and Privacy

Identity Management, Authentication, and Authorization

Cryptography and Secure Protocols

Risk and Security Management

Miscellaneous

Fifth International Workshop on Frontiers in Availability, Reliability, and Security (FARES 2010)

Fraud and Misuse Detection

Intrusion Detection

Privacy and Trust

Global Information Security

Software Security and Authentication

Digital Content Security

The Second International Workshop on Organizational Security Aspects (OSA 2010)

Organizational Aspects of Security: Session 1

Organizational Aspects of Security: Session 2

Organizational Aspects of Security: Session 3

Organizational Aspects of Security: Session 4

Fourth International Workshop on Secure Software Engineering (SecSE 2010)

Agile Development and Hot Patching

Testing, Monitoring, and Validation

Security Modeling and Vulnerabilites

Fourth International Workshop on Secure Systems Methodologies Using Patterns (SPattern 2010)

SPattern Application

SPattern Development

Fourth International Workshop on Advances in Information Security (WAIS 2010)

Identity and Privacy

System Security

Experimental and Physical Security

Third International Workshop on Digital Forensics (WSDF 2010)

Digital Forenisc Workshop: Session 1

Digital Forenisc Workshop: Session 2

Digital Forenisc Workshop: Session 3

Digital Forenisc Workshop Session 4

2010 International Conference on Availability, Reliability and Security

Managing the asset risk of SMEs

Luís Enrique Sánchez, Carlos Ruiz
Department of R+D
SICAMAN Nuevas Tecnologías
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain
{Lesanchez, Carlos}@sicaman-nt.com

Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. TSI Department
University of Castilla-La Mancha (UCLM)
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract— **The information society is becoming increasingly dependent on systems for managing and analysing the risk to which its main information assets are exposed and having access to these systems has become vital for the evolution of SMEs. However, this type of company requires the systems to be adapted to their special characteristics and to be optimised from the point of view of resources required to set them up and maintain them. This article presents a proposed method for carrying out risk analysis adaptation, which is suitable for SMEs, set within the framework of the methodology for security management in small and medium-sized enterprises (MSM2-SME). This model is being applied directly to real cases, and therefore its application is constantly being improved.**

SME; Management Risk, Asset; ISMS

INTRODUCTION

Studies conducted [1] have shown that, in order for companies to use information and communication technologies with guarantees, it is necessary to have the guides, metrics and tools that enable them to know their security level at all times and the vulnerabilities which are yet to be covered. The problem of ascertaining the risk to which a company's main assets are exposed is more marked in small and medium-sized enterprises, which have the additional limitation of insufficient human and economic resources to adequately manage their assets [2].

But with the arrival of the internet, it is becoming increasingly critical for companies to implement security controls that enable them to know and control the risks to which they may be exposed [3]. A large part of this change in mentality within companies stems from the social change brought about by the internet and the speed with which information is exchanged, which has led to a greater awareness among companies of the value of information for their organisation and to companies ensuring they protect their data. In this way, companies have already taken on board the fact that the information and processes that support their systems and networks are their most important assets [4]. These assets are exposed to a wide variety of risks which could have a critical effect on the company. The importance of security in information systems is backed up by numerous studies [5-7], to cite just a few.

Some authors [8, 9] suggest conducting a risk analysis as a fundamental part of security management in SMEs, since the owners of these assets should be aware that the value and sanction of the stolen or filtered data in a small organisation is the same as it is in a large organisation and, consequently, they should monitor the value and the risks to which these assets are exposed. Other authors [10] suggest the need to develop a new risk analysis model (RA) aimed directly at SMEs, given that the characteristics of these enterprises are different from those of large companies. This new model should take into account the fact that the uses of risk analysis and management techniques, and the role of third parties, are necessary to guarantee the security of the SME's information system.

Studies centred on risk evaluation [11-13], carried out on organisations in Europe and the USA, show that SMEs are characterised by insufficient dedication to the security of information technologies, due to the fact that these responsibilities are assigned to staff who do not have the right training. Likewise, the majority of organisations do not have security policies and risk evaluation systems, with 73% of UK SMEs interviewed saying they carry out risk evaluations in house. Less than 10% of those interviewed said that they use a risk analysis tool and none used a reference guide such as the ISO/IEC17799 [14]. This, together with the small number of organisations who really employ security specialists, leads to doubts over the exhaustiveness or effectiveness of the analysis they conduct.

As such, one of the issues arising from the conclusions is the need to come up with new methodologies and risk analysis and management models which are adapted to the particular characteristics of SMEs [15], in order to eliminate (or at least reduce) the problems and help these companies to evaluate the risks to which their assets are exposed and to establish suitable security controls.

Consequently, considering that SMEs account for a large majority of companies both at a national and international level and are a very important part of the business fabric of any country, [16] we believe it could be highly beneficial to conduct more research in order to improve the risk analysis and management processes for this type of company. This could contribute to improvements not only in the security of SMEs, but also in their competitiveness levels. For this reason, over the last few years we have been working on devising adapted process that enables the security risk of SMEs to be analysed and managed [17, 18], and we have also developed a tool that completely automates this process [19], and we have applied it in real cases [20], which has enabled us to validate both the methodology and the tool.

978-0-7695-3965-2/10 $26.00 © 2010 IEEE
DOI 10.1109/ARES.2010.52

In this paper, we present a zoom of the RAM (Risk Analysis and Management) for a comprehensive methodology (MSM2-SME) development and maintenance of SGSIs. The article continues in Section 2, with a brief description of the existing methodologies and models for analysing and managing security risk and current trends. In Section 3, we briefly introduce our proposed process for the analysis and management of security risk, aimed at SMEs, and it reusability of knowledge. In Section 4 we introduce the tools that support the risk analysis and management process, and we offer some of the results obtained when applying the process in a real case. Finally, in Section 5 we conclude by indicating the work that we will be undertaking in the future.

RELATED WORK

In order to fill some of the gaps highlighted in the previous section with regard to security management in companies, a large number of processes, work frameworks and methods for risk management have emerged and the need to use these to effectively protect a company's assets is increasingly being acknowledged and considered by organisations, but not yet in the case of SMEs.

Despite this, security management cannot be limited to the analysis and management of risk [21]. In addition to identifying and eliminating risks the process should also be carried out efficiently, leading to great cost savings for the company as a direct result of the improved security management [22]. Through risk analysis, assets can be identified and the level of security which needs to be applied can be ascertained.

The most prominent security management standards have included processes for risk analysis and management but these have proved difficult to apply in the case of SMEs as they require a large investment and are difficult to manage [23]. The main proposals for risk analysis and management include MAGERIT [24], OCTAVE [25] and CRAMM [26].

On the other hand, some of the main security management standards have tried to incorporate risk analysis and management into their processes:

- ISO/IEC27005 [27]: Establishes the guidelines for managing risk in information security. Supports the general concepts specified in regulation ISO/IEC27001 [28] and is designed to help with the satisfactory application of information security based on a risk management approach. Knowledge of the concepts, models, processes and terms described in regulation ISO/IEC27001 [28] and ISO/IEC27002 [29] is important to fully understand regulation ISO/IEC27005 [27].
- ISO/IEC21827/SSE–CMM [30]: A capable and mature model in the engineering of security systems, it describes the essential features of the process which a company must have in place in order to ensure a good level of security for their systems, including in the prior stages a process aimed at risk, with 4 sub-processes: SSE-PA02 (Determine the impact), SSE-PA03 (Identify security risks), SSE-PA04 (Identify threats), SSE-PA05 (Identify vulnerabilities).
- COBIT: This is a methodology for the suitable control of technology projects, information flows and the risks associated with not having appropriate controls. It includes a process for evaluating risks, in the domain PO9. This process centres mainly on criteria of confidentiality, integrity and availability and at a secondary level, on criteria of effectiveness, efficiency, compliance and reliability. Lastly, this process involves a number of profiles (Human Resources, Information, Technology, Installations and Data Systems) which form part of the information system.

There is also a small set of risk analysis tools. Currently the most widely used are PILAR and EAR, based on Magerit v2 [24]. Other tools used include the proposal from ENISA, which includes a comparative system, OCTAVE–S and Octave Automated Tool, which implement the risk evaluation methodology OCTAVE [25], CRAMM and COBRA.

The main problem with these processes and tools is the complexity for applying them to SMEs, since they have been conceived for use in large companies [31]. The excuse is often made [32, 33] that applying this type of process to SMEs is difficult and costly. Also, organisations, including large organisations, tend to adopt sets of related processes rather than dealing with processes independently [34].

Consequently, and as a conclusion to this section, we consider that it is pertinent and appropriate to tackle the problem of developing a new security risk management and analysis process for SME information systems, and a tool that supports this process, based on the problems that this type of company face which have led to continual failures in [35] attempts to introduce an ISMS in SMEs. A number of the most appropriate international regulations and documents will be used for this purpose, such as the security management guidelines ISO/IEC 13335 [36-38] and the MAGERIT [1] risk analysis and management methodology [24].

MANAGING ASSET RISK IN SMES

To resolve the problems detected in risk analysis and management when applied to SMEs, a new process has been developed aimed at managing risk in this type of company, called RAM-SME, which is part of the methodology for implementation and maintenance of safety management systems (MSM2-SME), which has two basic premises: i) it is aimed at SMEs; and ii) is focused on reducing the costs of generating and maintaining the risk analysis and management process.

This process has been reached by applying the action research method [39] and is set within the framework of the

[1] MAGERIT is the Spanish State Central Administration's risk management methodology, which is recognized by NATO (Military alliance of democratic states in Europe and North America).

methodology (MSM2-SME) [40] which covers all aspects of security management.

Within this methodology, the risk analysis and management process consists of two activities:

- Activity I: A structure of relationships is established between the different elements involved in the risk analysis and the controls needed for security management. These relationships are established using knowledge acquired in the different implementations. This is stored in a structure called a schema, to be reused at a later date, reducing the production costs of this process.
- Activity II: By selecting the most suitable schema and identifying a small set of the main assets, you get a detailed map of the current situation (risk analysis) and a plan of recommendations on how to improve it (risk management).

In the first activity we constructed a "risk model" that stores knowledge and that can be instantiated and reused by other companies who share the same characteristics (size and business sector), using the activity two.

To properly understand this process it is important to understand the concept of a Schema. This is a structure made up of the main elements of an ISMS and the relationships that can be established between them, through the Know-How acquired in different implementations. This structure can be reused by a group of companies with common characteristics (same sector and size) based on the knowledge acquired with the implementation of the MSM2–SME methodology and subsequent refinements.

This section is divided into two subsections which correspond to the two activities involved in the process.

1.1. RAM-SME Activity 1: Risk analysis as part of a Schema .

The main objective of this activity is to select the elements needed to carry out a basic, low cost risk analysis (adapted to the requirements of SMEs) on the assets that make up the company's information system, in activities subsequent to the methodology,.

This activity is based on the conclusions obtained when the action research method is applied [39] to different case studies, which have enabled a high degree of correlation to be determined between the elements involved in a risk analysis and the relationships between them when applied to SMEs with similar characteristics (same sector and same size), making it possible to establish said relationships a priori, eliminating the cost of having to analyse them individually through a consultation. Even when there are differences between them, these differences are irrelevant with regard to the final configuration of the ISMS obtained for SMEs, given that this type of company priorities cost to get a highly accurate result.

Although risk analysis is one of the fundamental parts of regulation ISO/IEC27001 [28] and is described in detail in standard ISO/IEC27005 [27], the main objective of the risk analysis included in the methodology developed is to be as low-cost as possible whilst still getting a result of a sufficiently high quality.

In Figure 1 you can see the basic schema of inputs, tasks and outputs which make up this activity:

- *Inputs:* As an input you receive the knowledge of the group of security domain experts (EGD) obtained during the process of implementing ISMSs, and also a set of controls for managing security which are stored in the schema repository and a set of elements needed to produce the risk analysis.
- *Tasks:* The sub-process consists of eight tasks which will be analysed in detail further on.
- *Outputs:* The output brought about by this sub-process is a subset of the input elements and the relationships established between them, which will be stored in the schema repository and which make up a third of the elements of the schema being generated.

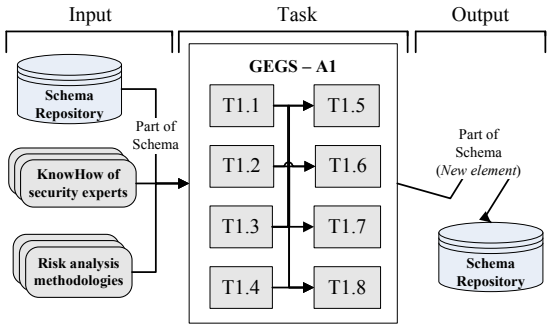

Figure 1. Simplified schema for activity A1 task.

Now we shall analyse the different tasks in the process that involve the different elements of the risk analysis.

- *Task T1.1 – Selecting types of assets:* This involves selecting the set of asset types that will form part of the schema being constructed. The asset types will then be used for a number of tasks: i) to group the information system assets; ii) they will be linked up with other risk analysis elements to enable this process to be automated.
- *Task T1.2 – Selecting threats:* This involves selecting the set of threats that will form part of the schema being constructed. A threat is defined as an event that could lead to an incident in the organisation, producing material damage or immaterial losses in its assets [24]. In subsequent tasks, these threats will be linked up with other risk analysis elements, with the aim of automating the process and reducing costs when evaluating the risks to which the assets of an information system are exposed.
- *Task T1.3 – Selecting vulnerabilities:* This involves selecting the set of vulnerabilities that will form part of the schema being constructed. A vulnerability is defined as a weakness or control fault that could result in a threat attacking an asset in the system in which the weakness has been identified [24]. In

subsequent tasks, these vulnerabilities will be linked up with other risk analysis elements, with the aim of automating the process and reducing costs when evaluating the risks to which the assets of an information system are exposed.

- *Task T1.4 – Selecting risk criteria:* This involves selecting the set of risk criteria that will form part of the schema being constructed. Risk criteria are defined as those criteria that enable an estimate to be made of the likelihood of a threat materialising in one or more assets causing damage to the organisation. In subsequent tasks, these risk criteria will be linked up with other risk analysis elements, with the aim of automating the process and reducing costs when evaluating the risks to which the assets of an information system are exposed.
- *Task T1.5 – Establishing relationships between asset types and vulnerabilities:* This involves establishing the relationships that exist between the elements that make up the set of asset types and the elements that make up the set of vulnerabilities for a particular schema.
- *Task T1.6 – Establishing relationships between threats and vulnerabilities:* This involves establishing the relationships that exist between the elements that make up the set of threats and the elements that make up the set of vulnerabilities for a particular schema.
- *Task T1.7 – Establishing relationships between threats and controls:* This involves establishing the relationships that exist between the elements that make up the set of threats and the elements that make up the set of controls for a particular schema.
- *Task T1.8 – Establishing relationships between asset types, vulnerabilities and risk criteria:* This involves establishing the relationships that exist between the elements that make up the set of asset types, the elements that make up the set of vulnerabilities and the elements that make up the set of risk criteria for a particular schema.

  The associations of tasks T1.5-8 are established by a group of domain experts (EGD) based on the knowledge acquired through different ISMS implementations.

1.2. RAM-SME Activity 2: Applying the risk analysis.

The main aim of this activity is to establish an evaluation of the risks to which the main assets of the information system of the company wishing to set up the ISMS are exposed, and to propose a plan to the head of security (Cu/RS) for managing the risk in the most efficient way.

In Figure 2 you can see the basic schema of inputs, tasks and outputs which make up this activity:

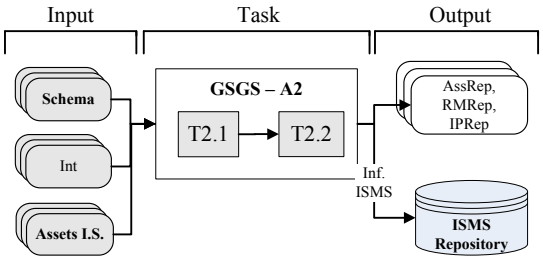

Figure 2. Simplified schema for activity A2 task.

- *Inputs:* As an input you will receive: i) a schema from the schema repository, which will be selected by the security consultant (SCo) based on the characteristics of the company (sector and size), from which the elements needed to carry out the risk analysis will be obtained; ii) the elected delegate for the company, who will be responsible for defining the assets; iii) a set of assets from the information system, as general as possible (course grain).
- *Tasks:* The sub-process consists of two tasks which will be analysed in detail further on.
- *Outputs:* The output produced by this sub-process will be a series of handouts (report on information system assets, matrix of risks to which the information system assets are exposed and the improvement plan recommended by the methodology for tackling the ISMS security management improvements) so that the security consultant (SCo) can analyse them. The information found in these handouts will be stored in the ISMS repository to be used at a later date to generate the elements that make up the company's ISMS.

This activity is based on the Stephenson proposal [41] which centres on the synergy between the technical test and the risk analysis, taking ISO/IEC27002 as a reference[29] and on the risk analysis methodology Magerit v2 [24]. These methodologies are often rejected by SMEs as they are seen as too complex and requiring a huge commitment on the part of the company members and the associated costs are not accepted by the SMEs. For this reason, the MSM2–SME methodology simplifies this risk evaluation process making it suitable for SMEs.

The defining principles of this activity include the following: flexibility, simplicity and cost efficiency (human and time-related). It is therefore an activity which attempts to identify the company's assets and associated risks in the most cost-effective way possible, using the results generated in previous activities and some simple algorithms.

The risk analysis part of the methodology takes some aspects from Magerit v2 [24] and some from classic risk analyses, but at all times tends towards simplification.

In order for this activity to operate coherently, the special conditions of SMEs need to be taken into account, such as the fact that the users do not usually have the time or appropriate knowledge to efficiently apply risk analysis methodologies or to adequately determine the assets of their information systems.

As in the previous activity, when it comes to SMEs, it is not the optimal option which is sought but rather a good reasonable option which allows for a significant reduction in the time it takes to obtain the result.

The tasks for this activity are mainly supported by the data which makes up the selected schema, generated in activity A1 and by a list of security controls.

Below we offer a detailed look at the tasks which make up this activity:

- *Task T2.1 – Identifying assets:* The aim of this task is to obtain a set of the assets that make up the company's information system. The ISMS is focused on the assets defined as these are the elements which it is intended to protect, because they are of value to the company and, in most cases, are the distinguishing factor in terms of competitiveness.

  One of the main differences offered by the method for risk evaluation in the methodology is that it tries to make sure the assets are as general as possible (course grain), rather than [24] trying to identify them clearly and precisely (fine grain).

  For SMEs attempts should be made to identify a very small and basic set of assets, since their information systems do not permit the discriminate protection of assets which cannot be easily fragmented and they cannot support the cost of managing these assets. Therefore, this task looks for general assets which are simple to value from both a quantitative and qualitative point of view.

  In this task the security consultant (SCo) should help the elected delegate to identify the set of valuable assets that make up the company's information system.
- *Task T2.2 – Generating the risk matrix and improvement plan:* The aim of this task is to carry out an evaluation of the risks to which the assets of the company, defined in task T2.1, are exposed.

  The data generated in activity A1 and the assets identified in task T2.1 are required in this task to generate a risk matrix which gives a detailed account of the risks to which each asset is exposed and an improvement plan that determines how these risks are to be tackled.

  The improvement plan is supported by the results obtained in the risk matrix. The risk matrix and the improvement plan are used by the security consultant (SCo) to determine and analyse additional and urgent measures which the company should take in order to mitigate high-level risks to the company's information assets.

  The first aim of this task is to generate a risk matrix that enables us to find out what risks each of the company's assets are exposed to at each level of maturity and for each risk assessment element (threats, vulnerabilities and risk criteria). The result will be a table with the following columns:
  - Level: Security maturity level.
  - Name and description of asset.
  - Cost of asset: quantitative value that the loss of the asset would have for the company.
  - Strategic value: qualitative value that the loss of the asset would have.
  - Asset type.
  - Threat.
  - Vulnerability.
  - Risk criteria.
  - Level of threat (LT): This is determined by taking into account the impact that a threat would have on an asset. The scale values range from [low = 1, medium = 2, high =3];
  - Probability level (P): This is defined as the probability of occurrence of a vulnerability based on the empirical criteria. The scale values range from [low = 1, medium = 2, high =3];
  - Risk level (RL) (see equation 1): The definition of the risk level (RL) is obtained from the probability (P) of occurrence (vulnerability) and the threat level (LT).

$$RL = P * LT \quad (1)$$

With:

- RL: Risk level.
- P: Probability of occurrence of the vulnerabilities.
- LT: Threat level.

  - Level of control or coverage: This is the compliance level of a security control in relation to a particular asset, exposed to a threat at a particular maturity level (see equations 2 and 3). This data is essential in order to come up with an improvement plan, since the system will use this data to plan the order in which the controls should be improved in order to minimise risks.

$$NCCAA(x,y,z) = \Sigma\ (VACAM)/NCAM \quad (2)$$

With:

- NCCAA: Level of coverage that the controls in the system currently offer to asset X against threat Y in relation to security level Z.
- NCAM: Number of controls affected by the threat for that maturity level.
- VACAM: Current value of the control affected by the threat for each of the maturity levels.

$$NCCA = \Sigma(NCCAA)/\ NAA \quad (3)$$

With:

- NCAA: Level of coverage offered by the current controls in the system for asset X against any threat.
- NCCAA: Level of coverage that the controls in the system currently offer to asset X against threat Y in relation to security level Z.
- NAA: With NAA being the number of threats that affect the asset.

The value obtained for risk level (RL) will be managed in accordance with Table I and will range between 1 (lowest risk) and 7 (highest risk). It has been determined that the residual risk level (RRL), that is, the level the company currently has, will never be greater than the acceptable risk level (ARL), which is the level the company should be aiming towards. For the RAM-SME process it is considered that the ARL should be less than or equal to 3. If the RL is greater than the ARL, safeguards are then selected to reduce the risk, and the process is carried out resourcefully until the company reaches the right risk level.

TABLE I. TABLE FOR DETERMINING RISK LEVEL.

ARL=<3	LT	Low			Medium			High		
	P	L	M	H	L	M	H	L	M	H
Asset value	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

To ascertain the risk to which each asset is exposed and the coverage level of each control in a simple way, the Risk Matrix (RMa) algorithm will be used (see Table II).

TABLE II. PSEUDOCODE OF THE RISK MATRIX ALGORITHM.

Algorithm: Risk matrix.

Given a Schema, Company, ISMS and ISMS Application.

1.– Ascertain the coverage level of each security control.

2.– Ascertain the impact of the threats for each asset and level.

3.– Ascertain the probability of occurrence of a vulnerability on an asset and maturity level.

4.– Obtain the risk matrix to ascertain the risk level for each asset.

Once you have the risk matrix, this will be used - together with the information generated in the previous tasks - to work out the improvement plan, through the application of the Improvement Plan algorithm (aPM) (see Table III). This algorithm operates resourcefully, determining the asset with the highest risk level at the lowest maturity level and applying the control that enables this to be improved at the lowest cost. It then recalculates the whole process and selects the next best option until reaching the optimal security management level.

TABLE III. PSEUDOCODE OF THE IMPROVEMENT PLAN ALGORITHM.

Algorithm: Improvement plan.

Given a Schema, Company, ISMS and ISMS Application.

1.– When the risk level is higher than the assumable risk

1.1.– The risk matrix is recalculated with ascending maturity level and descending risk level.

1.2.– The first record on the matrix is selected.

1.3.– The controls for that matrix record are obtained.

1.4.– The control with the lowest coverage level is selected.

1.5.– It issues the full recommendation of the improvement that compliance with the control would result in.

1.6.– The matrix is recalculated and the weights are updated.

TOOL AND ITS APPLICATION IN REAL CASES.

An application has been developed which is able to support the risk analysis and management process, designed for SMEs. This application is divided into two zones, which provide support to each of the activities in the RAM-SME process.

Within the management zone of the application's schema is the "risk analysis" management, which enables the different components of the basic risk analysis to be configured by adding or removing new elements to or from these components. This zone corresponds to the first activity in the RAM process.

Because it is based on the developed methodology, the only notable task involved in carrying out the risk analysis is to enter the company's information system assets, which must be quantified. This zone corresponds to the second activity in the RAM-SME sub-process.

Using the assets and the results obtained for the control compliance levels with ISO/IEC27002, the model generates a complete risk matrix for the company totally automatically, so that the head of security can have a complete map of risks, vulnerabilities, threats and coverage level for each of the assets that make up the company's information system.

The matrix generated by the MSM2–SME model for the real case of the company Sicaman Nuevas Tecnologías (SNT) includes 711 records. The risk matrix includes detailed information on the assets for each maturity level and on how these are affected according to asset type, the threats to which these assets are exposed, vulnerabilities and risk criteria which have been taken into account for this asset. Using this information, the impact of each threat on an asset and the probability of occurrence of each vulnerability are assessed. This enables a risk level to be established which will be associated to the company's control level to determine how to tackle an improvement plan.

Using the risk matrix, the system is able to devise an improvement plan and propose a series of steps to increase

the company's security level in the shortest time-scale. Table IV shows the first step proposed in the improvement plan, for the case study. In the case of SNT, the system requires 48 steps to reach an acceptable risk level for the company's information system. Because of limited space, only the first step of the improvement plan is shown.

TABLE IV. IMPROVEMENT PLAN FOR SNT.

Step 1: The company's current level is level 1 with a maximum risk of 6 at this level. The asset most affected by the risk is: hardware (servers) the loss of which would cost the organisation 50,000 euros and the strategic value of which for the company is 3 over 7, with the asset type being "hardware". The risk level for this asset for the threat "hardware failure (physical device)" is 6 and the system currently has a control coverage level of 0.21, for which reason it is recommended that control activation is tackled [10.5.1] (copies of information security.). …

CONCLUSIONS

In this article we have presented the proposal for a process to carry out risk analysis and management in SMEs, called RAM-SME, which enables the results generated during the investigation to be supported and the desired objectives to be met.

The generation and maintenance cost of risk analysis for SMEs should be very low, even if this means sacrificing the accuracy of the analysis, but the results should always be of a sufficiently high quality.

We have defined how this process and the improvements it offers can be used as compared to other models that tackle the problem in a more precise and detailed, but also more costly, way, making them unsuitable for SMEs.

The features offered by the process and its orientation towards SMEs have been very well received and its application is proving to be very positive as it enables this type of company to adequately manage the risks to which their information system assets are exposed. Furthermore, this process provides short term results and reduces the costs that the use of other processes entail, achieving higher satisfaction levels within the company.

The RAM-SME process meets the proposed objectives and complies with the principles that, according to the Organisation for Economic Co-operation and Development (OECD) [42] all risk evaluation processes must follow. This means that the system must be able to continually self-evaluate risk and propose measures.

Finally, it is considered that the work carried out should be extended, with new specifications, new schemas, improvements to the risk analysis and management algorithms, enabling them to offer more detailed plans and a more in-depth look into the process with new case studies.

Most of the future improvements to the process are aimed at improving accuracy, but always respecting the principle of resource costs, that is, seeking to improve the process without incurring risk analysis generation and maintenance costs.

ACKNOWLEDGMENT

This research is part of the following projects: BUSINESS (PET2008-0136) granted by the "Ministerio de Ciencia e Innovación" (Spain), QUASIMODO (PAC08-0157-0668) project financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", SISTEMAS (PII2I09-0150-3135) project financed by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha" and MEDUSAS (IDI-20090557) project financed by the "Centro para el Desarrollo Tecnológico Industrial. Ministerio de Ciencia e Innovación"(CDTI).

REFERENCES

[1] Wiander, T. Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. in AISC '08: Proceedings of the sixth Australasian conference on Information security. 2008. Wollongong, Australia.

[2] Wiander, T. and J. Holappa, Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor. 2006.

[3] Dhillon, G. and J. Backhouse, Information System Security Management in the New Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.

[4] Kluge, D. Formal Information Security Standards in German Medium Enterprises. in CONISAR: The Conference on Information Systems Applied Research. 2008.

[5] Hall, A. and R. Chapman, Correctness by Construction: Developing a Commercial Secure System. IEEE Software, 2002. 19(1): p. 18-25.

[6] Masacci, F., M. Prest, and N. Zannone, Using a security requirements engineering methodology in practice: The compílanse with the Italian data protection legislation. Computer Standards & Interfaces, 2005. 27: p. 445-455.

[7] Walker, E., Software Development Security: A Risk Management Perspective. The DoD Software Tech. Secure Software Engineering, 2005. 8(2): p. 15-18.

[8] Volonino, L. and S. Robinson. Principles and Practice of Information Security. in 1 edition, Anderson, Natalie E. 2004. New Jersey, EEUU.

[9] Michalson, L., Information security and the law: threats and how to manage them. Convergence, 2003. 4(3): p. 34-38.

[10] Spinellis, D. and D. Gritzalis. Information Security Best Practise Dissemination: The ISA-EUNET Approach. in WISE 1:First World Conference on Information Security Education. 1999.

[11] Dimopoulos, V., et al. Approaches to IT Security in Small and Medium Enterprises. in 2nd Australian Information Security Management Conference, Securing the Future. 2004b. Perth, Western Australia: 73-82.

[12] Holappa, J. and T. Wiander, Practical Implementation of ISO 17799. Compliant Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor. 2006.

[13] Llvonen, L. Information Security Management in Finnish SMEs. in 5th European Conference on Information Warfare and Security National Defence College. 2006. Helsinki, Finlan: 1-2 June 2006.

[14] ISO/IEC17799, ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management. 2000.

[15] Taylor, M. and A. Murphy, SMEs and eBusiness. Small Business and Enterprise Development, 2004. 11(3): p. 280-289.

[16] Tawileh, A., J. Hilton, and S. McIntosh, Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach, in ISSE/SECURE 2007 Securing Electronic Business Processes, Vieweg, Editor. 2007. p. 331-339.

[17] Sánchez, L.E., et al. Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799. in International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES. 2006. Viena (Austria).

[18] Sánchez, L.E., et al. Developing a model and a tool to manage the information security in Small and Medium Enterprises. in International Conference on Security and Cryptography (SECRYPT'07). 2007a. Barcelona. Spain.: Junio.

[19] Sánchez, L.E., et al. SCMM-TOOL: Tool for computer automation of the Information Security Management Systems. in 2nd International conference on Software and Data Technologies (ICSOFT'07). . 2007c. Barcelona-España Septiembre.

[20] Sánchez, L.E., et al. Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas. in International Conference on Security and Cryptography (SECRYPT'08). 2008. Porto–Portugal.

[21] Siegel, C.A., T.R. Sagalow, and P. Serritella, Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Security Management Practices, 2002. sept/oct: p. 33-49.

[22] Garigue, R. and M. Stefaniu, Information Security Governance Reporting. Information Systems Security, 2003. sept/oct: p. 36-40.

[23] Bohemer, W. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. in SECURWARE '08: Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies. 2008.

[24] MageritV2, Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2). 2006, Ministerio de Administraciones Públicas (Spain).

[25] Alberts, C.J. and A.J. Dorofee, Managing Information Security Risks: The OCTAVE Approach., ed. A.-W.P. Co. 2002.

[26] CRAMMv5.0, CRAMM v5.0, CCTA Risk Analysis and Management Method. 2003.

[27] ISO/IEC27005, ISO/IEC 27005, Information Technology - Security Techniques - Information Security Risk Management Standard (under development). 2008.

[28] ISO/IEC27001, ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements. 2005.

[29] ISO/IEC27002, ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management. 2007.

[30] ISO/IEC21827, ISO/IEC 21827:2002, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM). 2002, ISO/IEC. p. 123.

[31] Batista, J. and A. Figueiredo, SPI in very small team: a case with CMM. Software Process Improvement and Practice, 2000. 5(4): p. 243-250.

[32] Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.

[33] Tuffley, A., B. Grove, and M. G, SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.

[34] Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.

[35] Fomin, V.V. and H. Vries. ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption. in EuroMOT 2008 - The Third European Conference on Management of Technology. 2008. Nice, France.

[36] ISO/IEC13335-3, ISO/IEC TR 13335-3, Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security. 1998.

[37] ISO/IEC13335-4, ISO/IEC TR 13335-4, Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards. 2000.

[38] ISO/IEC13335-5, ISO/IEC TR 13335-5, Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security. 2001.

[39] Kock, N., The threee threats of action research: a discussion of methodological antidotes in the context of an information systems study. , in Decision Support Systems. 2004. p. 265-286.

[40] Sánchez, L.E., et al. MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. in 9th International Conference on Enterprise Information Systems (WOSIS'07). 2007b. Funchal, Madeira (Portugal). June.

[41] Stephenson, P., Forensic Análisis of Risks in Enterprise Systems. Law, Investigation and Ethics, 2004. sep/oct: p. 20-21.

[42] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security., O.f.E.C.-o.a.D. (OECD). Editor. 2002: Paris.